RSAC™ | 2025 Conference

Many Voices.
One Community.

SESSION ID: PART1-W09

The New Attack Frontier: Research Shows Apps & APIs are the Targets

Rupesh Chokshi

SVP & GM, Application Security
Akamai Technologies

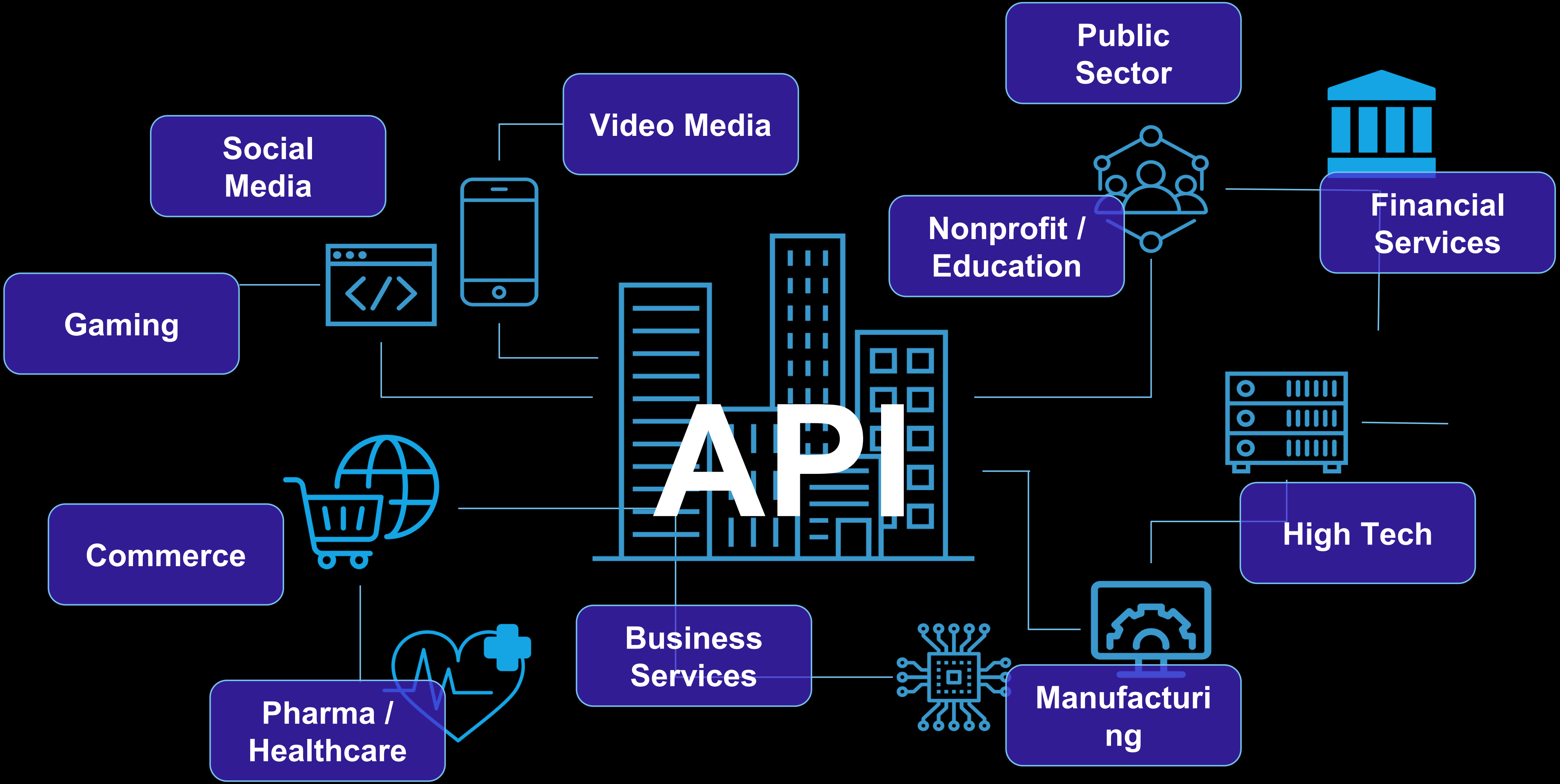
Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.

APIs Are Everywhere…



Public Sector
Video Media
Social Media
Nonprofit / Education
Financial Services
Gaming
API
High Tech
Commerce
Business Services
Manufacturing
Pharma / Healthcare

…and Securing Applications Is Harder Than Ever

5.8B
Users on the Internet

75B
IoT Devices by 2025

8.9M
Mobile Applications Downloaded Worldwide

30
Average apps downloaded and used by users each month

17
Average connected devices per household

7.4M
ChatGPT app downloads in first 10 days of launch

991
Average Apps Per Enterprise

With applications running your business, vulnerabilities multiply as the ecosystem becomes more complex.

Resulting in an ever-growing attack surface.

Our journeys to this conference used possibly thousands of APIs…

Book Hotel
& Airfare

Order
a Car

Order Coffee
on an App

Log in to
Social Media

Check the
Weather

Check in for
a Flight

Use Google
Maps

Eat at a
Restaurant

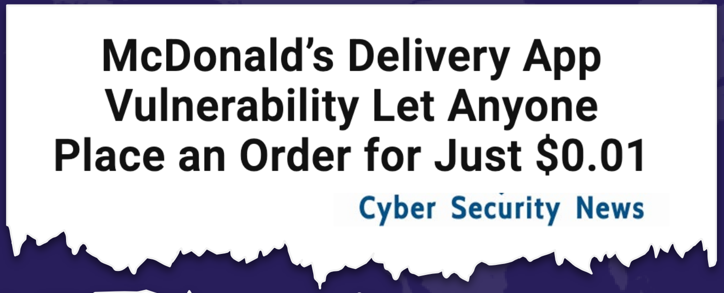
…and they’re under attack

150,000,000,000

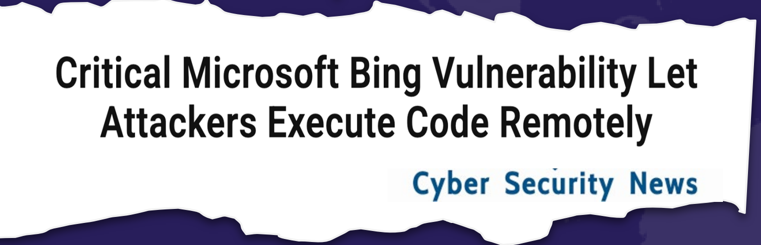
of web attacks targeted APIs

January 2023 - December 2024

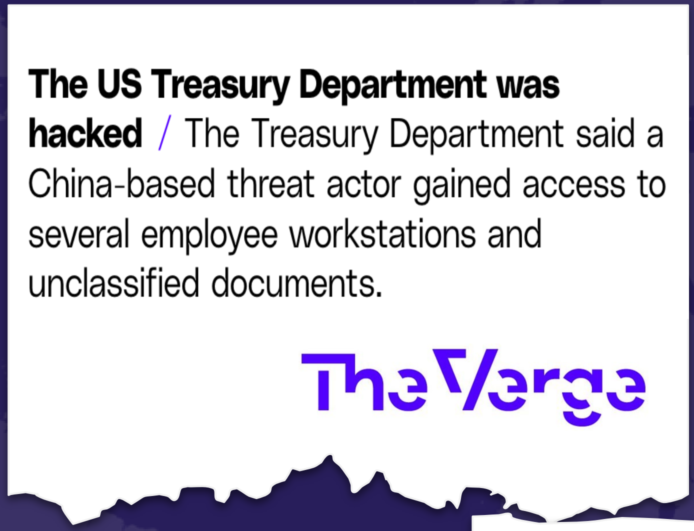
APIs: The Attackers' Favorite Target


McDonald's Delivery App Vulnerability Let Anyone Place an Order for Just $0.01

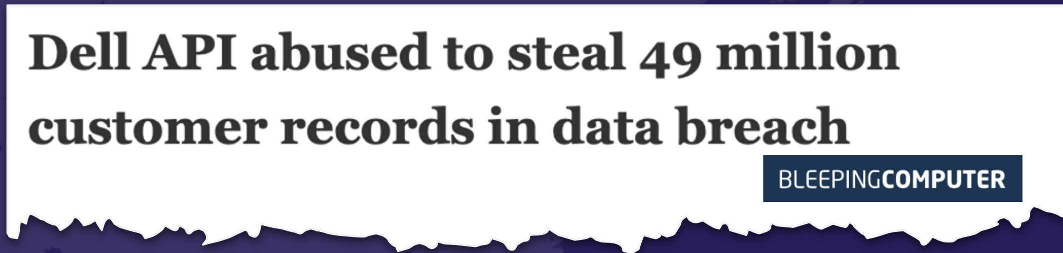
Cyber Security News


Critical Microsoft Bing Vulnerability Let Attackers Execute Code Remotely

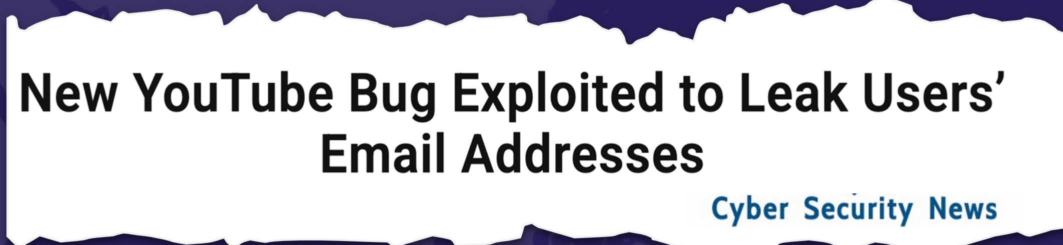
Cyber Security News


The US Treasury Department was hacked / The Treasury Department said a China-based threat actor gained access to several employee workstations and unclassified documents.

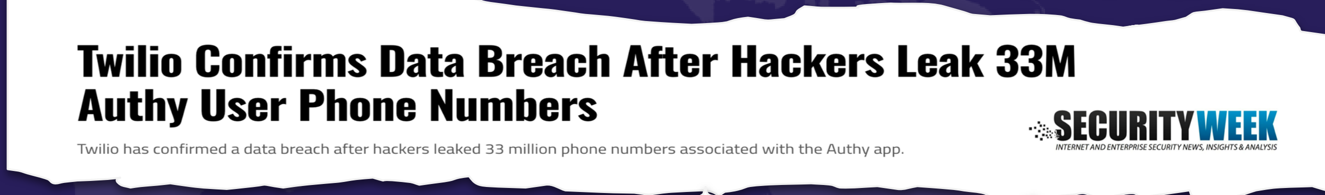
The Verge


Dell API abused to steal 49 million customer records in data breach

BLEEPINGCOMPUTER

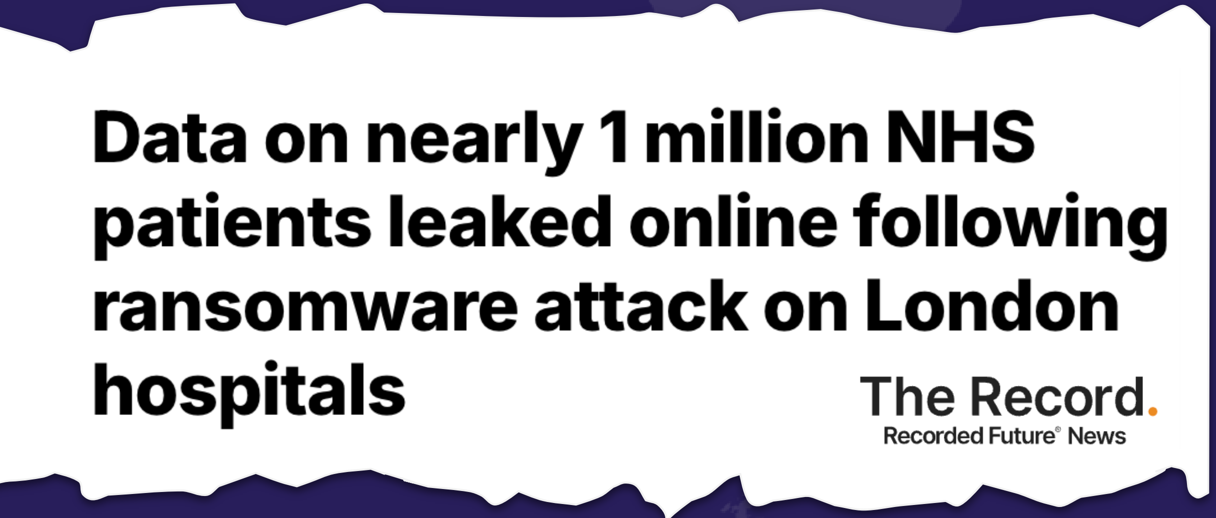

New YouTube Bug Exploited to Leak Users' Email Addresses

Cyber Security News

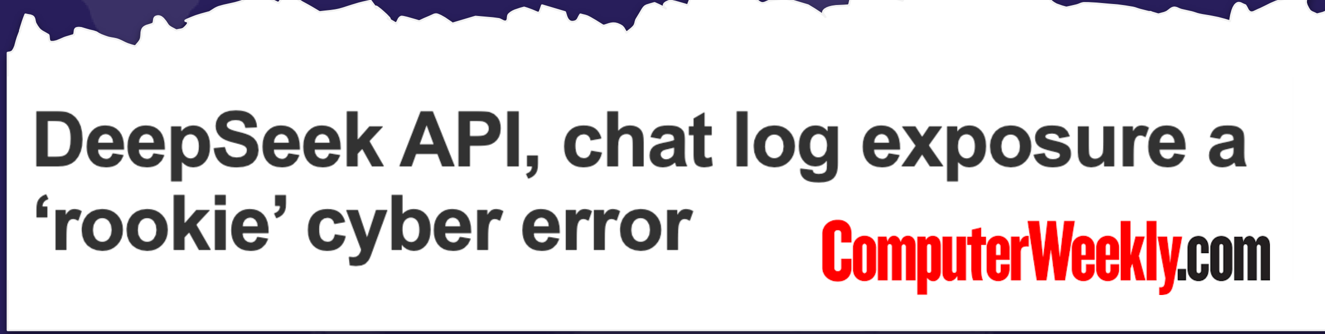

Twilio Confirms Data Breach After Hackers Leak 33M Authy User Phone Numbers

Twilio has confirmed a data breach after hackers leaked 33 million phone numbers associated with the Authy app.

SECURITY WEEK
INTERNET AND ENTERPRISE SECURITY NEWS, INSIGHTS & ANALYSIS


Data on nearly 1 million NHS patients leaked online following ransomware attack on London hospitals

The Record.
Recorded Future® News


DeepSeek API, chat log exposure a 'rookie' cyber error

ComputerWeekly.com

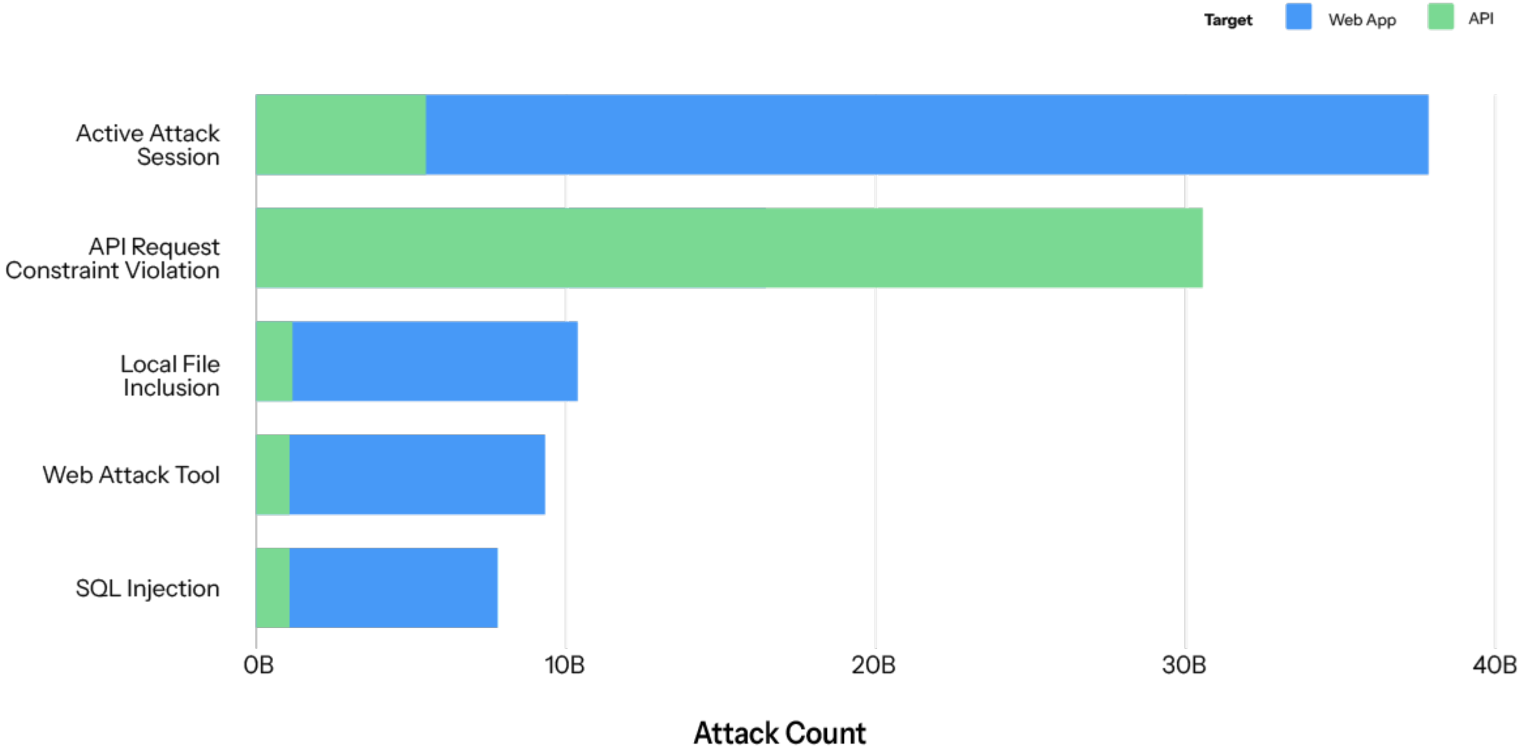
Web & API Attacks Are A Global Problem

116B

EMEA saw the highest percentage of API attacks globally at 37%

EMEA: Web Attacks by Vector

January 1, 2023 — December 31, 2024



Hijacked Telecom API Token Used Overseas Nearly Went Unnoticed

Missed Vulnerability:

A private API meant only for California-based resellers was accessed from a high-risk European IP using a hijacked JSON web token

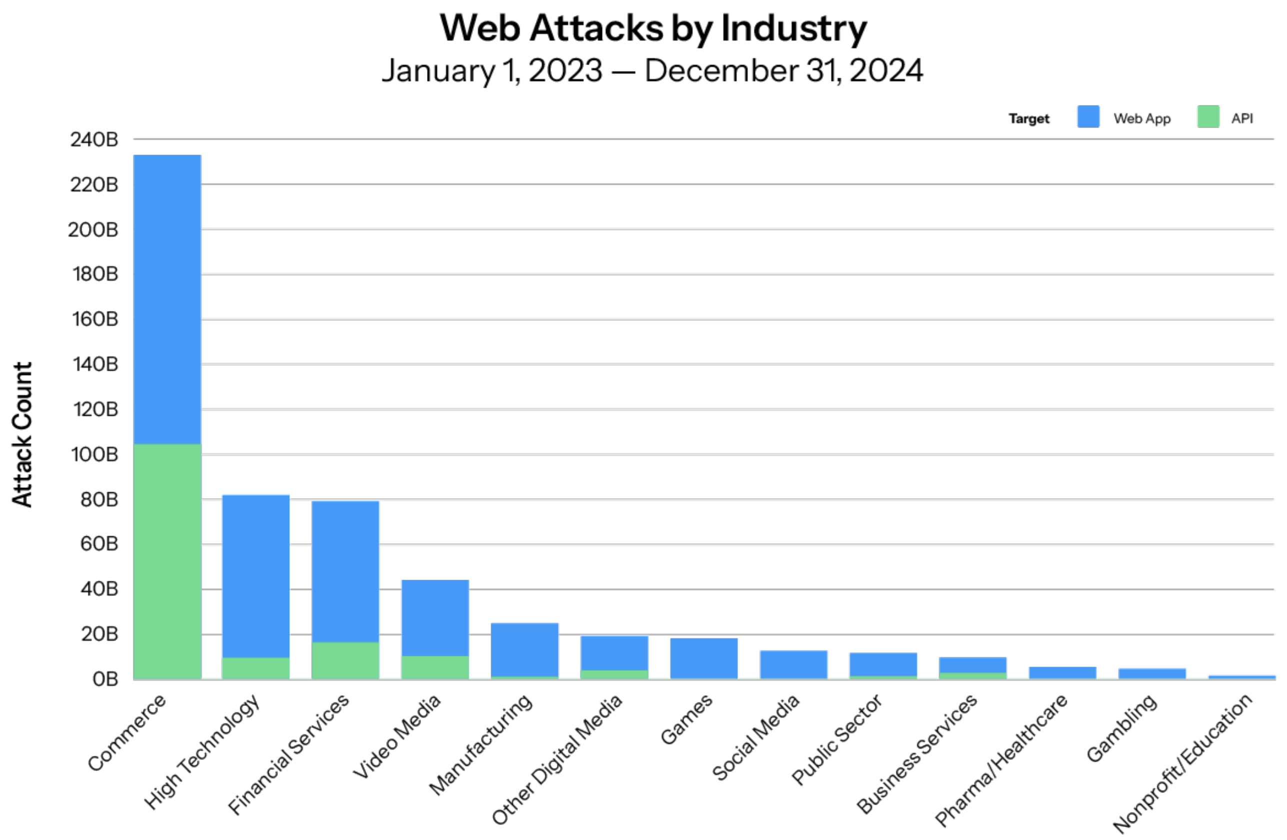
Impact:

A valid employee token was used to pull sensitive reseller reports—despite clear signs of abuse, including geo mismatch and risk-based indicators.

Who’s Under Attack?

230B+

web attacks hit **commerce** organizations from 2023-2024, nearly triple the number of attacks experienced by **high technology** (the second most attacked)



Web Attacks by Industry

January 1, 2023 — December 31, 2024

Retail Beverage Giant Missed One API Flaw, Nearly 100M Users At Risk

Missed Vulnerability:

No centralized API governance across global platforms—critical exposure went undetected.

Impact:

A publicly commissioned bug bounty uncovered a vulnerability exposing names, emails, phone numbers, and addresses of nearly **100 million users**.

AI-Driven Scraping Has Exploded

amkodor
211E
Claude
Gemini
deepseek

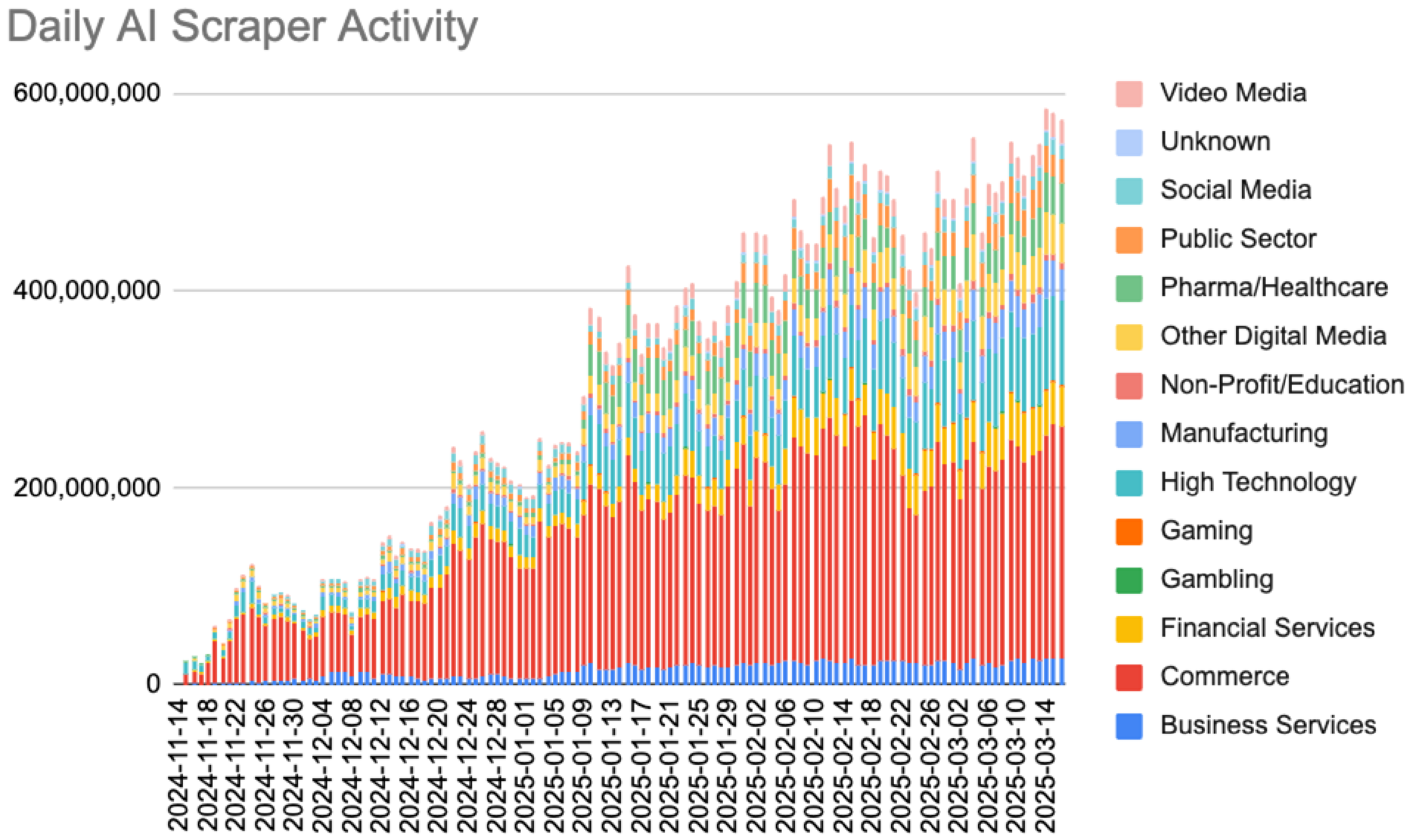
Our team sees

500M+

LLM scraping requests per day

Commerce at the Center of Early Scraping Activity

Dynamic inventories & pricing led to massive scraping spikes

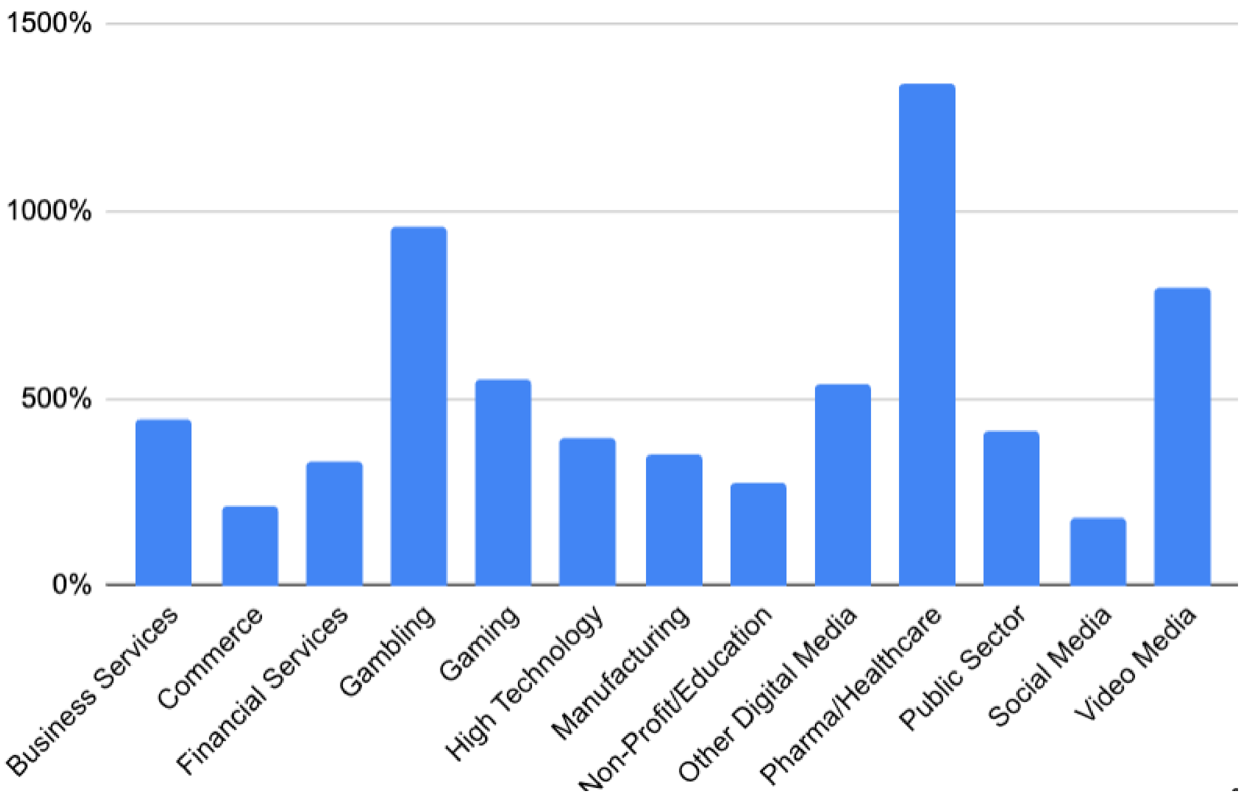


The Real Shock: Acceleration in Other Industries

Biggest Growth Sectors:

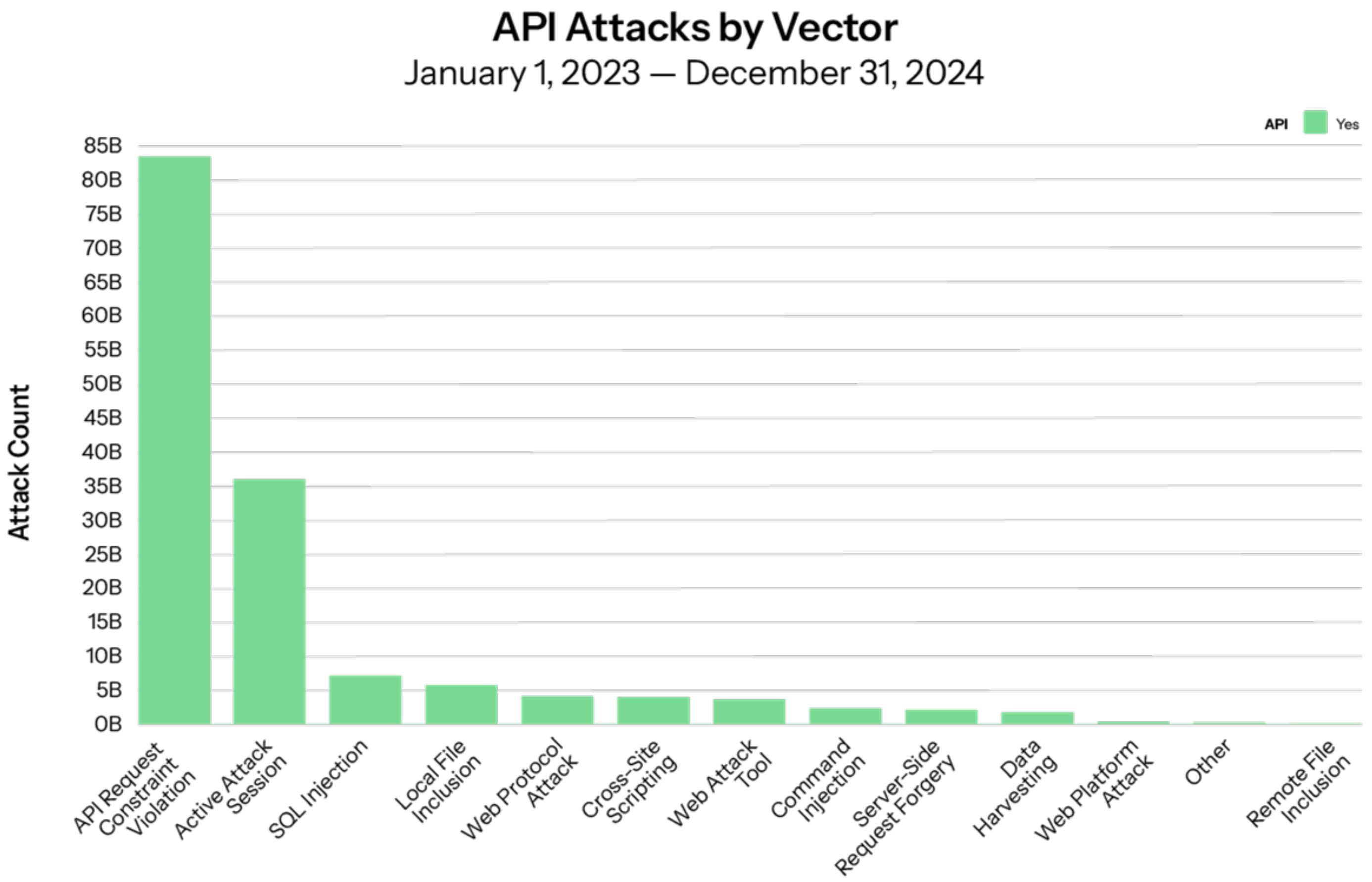
- Healthcare +1340%
- Gambling +957%
- Video Media +794%

LLM Scraping - January to March 2025 Change



Old Tactics, New Scale

API Request Constraint Violation and Active Attack Session are by far the most frequent vectors, vastly outweighing OWASP-style exploits like SQL injection or SSRF.



API Attacks by Vector

January 1, 2023 — December 31, 2024

Akamai

RSAC 2025 Conference

Security Gaps Across APIs, Applications, & AI

API Risks

- Shadow & Zombie APIs
- Business Logic Abuse (BOLA, BFLA)
- Unprotected APIs targeted by Bots & DDoS

App Risks

- Broken Authentication & Access Controls
- Code Injection
- Vulnerable Dependencies, Open Source Risk

LLM Risks

- LLM-Powered Scraping & Data Harvesting
- Automated Fake Account Creation & Fraud
- Model Manipulation & Prompt Injection Attacks

Where’s Your Weak Spot?

Three Questions to Ask

Visibility

Do you know which APIs, applications, and AI integrations you expose?

Security Posture

Are your APIs, applications and AI models protected against misuse and known vulnerabilities?

Abuse & Exploitation

Can you detect and prevent automated abuse, fraud, and business logic attacks?

Looking to the Future: Compliance

You cannot protect what you cannot see

The risks associated with a lack of visibility into a company's API and AI space create potentially serious legal and regulatory concerns

How to Protect Against Abuse

- Discovery
- Visibility
- Remediation

Your Application Security Action Plan

NEXT WEEK

Visibility & Control

Shine a Light in the Shadows: Find & document unmonitored APIs

Get Your House in Order: Organize your API inventory

WITHIN 3 MOS.

Strengthen & Defend

Harden API posture: Look at common alert types and identify strategies and priorities to reduce risk

Sharpen Your Threat Detection & Response: Create response plans to address possible attacks from adversaries

WITHIN 6 MOS.

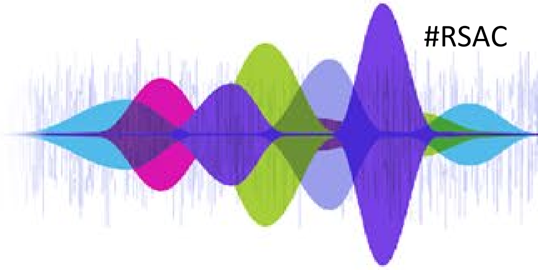
Proactively Mitigate

Think Like an Attacker: Conduct API security audits & penetration testing to simulate real-world threats

Develop a stronger offense: Establish a formal API threat hunting discipline

Learn more

Akamai State of the Internet Reports



#RSAC

SOTI
Lurking in the Shadows
Attack Trends Shine Light on API Threats

SOTI
Fighting the Heat
EMEA's Rising DDoS Threats

SOTI
Scraping Away Your Bottom Line
How Web Scrapers Impact Ecommerce

SOTI
Digital Fortresses Under Siege
Threats to Modern Application Architectures

SOTI
Navigating the Rising Tide
Attack Trends in Financial Services

SOTI
Healthcare Under the Microscope
Attacks Focus on Applications and APIs

SOTI
2024
The Year in Review

SOTI
Defenders' Guide 2025
Fortify the Future of Your Defense

SOTI
V11 ISSUE 02

State of Apps and API Security 2025
How AI Is Shifting the Digital Terrain

Akamai
State of the Internet/Security

The State of the Internet series provides expert insights on the cloud security landscape, based on data gathered from the Akamai Connected Cloud.

Get the latest report.

Akamai

RSAC 2025 Conference

RSAC 2025 Conference

Thank You

Many Voices.
One Community.